

Uniqueness of low genus optimal curves over \mathbb{F}_2

Alessandra Rigato

Abstract

A projective, smooth, absolutely irreducible algebraic curve X of genus g defined over a finite field \mathbb{F}_q is called *optimal* if for every other such genus g curve Y over \mathbb{F}_q one has $\#Y(\mathbb{F}_q) \leq \#X(\mathbb{F}_q)$. In this paper we show that for $g \leq 5$ there is a unique optimal genus g curve over \mathbb{F}_2 . For $g = 6$ there are precisely two and for $g = 7$ there are at least two.

1 Introduction

Let X be a projective, smooth and absolutely irreducible genus g curve defined over a finite field \mathbb{F}_q . It is well known that the number of \mathbb{F}_q -rational points of X is bounded and a lot of research has been done to determine whether the bounds are sharp: see for example Sections 5.2 and 5.3 of [Sti] for an overview. The curve X is called *optimal* if for every other genus g curve Y over \mathbb{F}_q one has $\#Y(\mathbb{F}_q) \leq \#X(\mathbb{F}_q)$. The main result of this paper deals with uniqueness up to \mathbb{F}_2 -isomorphism of small genus optimal curves defined over \mathbb{F}_2 .

Theorem 1.1. *For $g \leq 5$, there exists a unique optimal genus g curve defined over \mathbb{F}_2 . There exist two non-isomorphic genus 6 optimal curves and at least two non-isomorphic genus 7 optimal curves defined over \mathbb{F}_2 .*

Examples of small genus optimal curves defined over \mathbb{F}_2 are already present in [S], [S1] and [N-X]. In this paper we show that for genus $g \leq 5$ these examples are unique, while one of the genus 6 curves we construct appears to be new.

The proof of this result consists of two steps. We first determine a short list of Zeta functions that an optimal curve over \mathbb{F}_2 can have. In Section 2 we show that for genus $g \leq 5$ there is only one possible Zeta function, while for $g = 6$ there are two. Next we apply class field theory techniques as in [A], [L], [Sch], [S], [S1], and recent results by Howe and Lauter in [H-L] to show that for each possible Zeta function there exists precisely one curve. In Section 3 we discuss curves of genus 0 and 1. Sections 4 to 8 are devoted to curves of genus 2 to 6. Finally, in Section 9 we exhibit two optimal genus 7 curves with different Zeta functions.

The author wishes to express her gratitude to her advisor René Schoof, for this work would not have been possible without his precious help. The author also thanks Everett Howe for his interesting and constructive comments and Claus Fieker for his MAGMA computation. Part of this paper was written while the author was supported by the Fund for Scientific Research Flanders (F.W.O. Vlaanderen)

2 Zeta function and real Weil polynomial of a curve

Throughout this paper a curve is understood to be projective, smooth and absolutely irreducible over a finite field of definition \mathbb{F}_q . In order to study optimal genus g curves defined over \mathbb{F}_q it is of interest to determine the quantity

$$N_q(g) := \max\{\#X(\mathbb{F}_q) \mid X \text{ is a genus } g \text{ curve defined over } \mathbb{F}_q\}.$$

Then, an optimal genus g curve X defined over \mathbb{F}_q satisfies $\#X(\mathbb{F}_q) = N_q(g)$. Several methods have been developed in order to determine $N_q(g)$ for given q and g . The progress is listed and continuously updated in the tables [G-V]. In particular Serre determined very good upper bounds for the number of \mathbb{F}_q -rational points in [S1]. For $q = 2$ he gives the estimate $\#X(\mathbb{F}_2) \leq 0.83g + 5.35$. For $g \geq 2$ this improves the Hasse-Weil bound $\#X(\mathbb{F}_q) \leq q + 1 + \lfloor 2g\sqrt{q} \rfloor$. In [S] Serre also provided examples of genus g curves defined over \mathbb{F}_2 attaining these bounds. Hence for small genus curves he proved that $N_2(g)$ is as follows [S1, Theorem 5]

g	0	1	2	3	4	5	6	7
$N_2(g)$	3	5	6	7	8	9	10	10

The Zeta function of a genus g curve X defined over \mathbb{F}_q is given by

$$Z(t) = \prod_{d \geq 1} \frac{1}{(1 - t^d)^{a_d}},$$

where

$$a_d = \#\{P \mid P \text{ place of } X \text{ such that } \deg P = d\}.$$

In particular, $a_1 = \#X(\mathbb{F}_q)$. The Zeta function $Z(t)$ is a rational function of the form

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)},$$

where

$$L(t) = \prod_{i=1}^g (1 - \alpha_i t)(1 - \overline{\alpha_i} t)$$

for certain $\alpha_i \in \mathbb{C}$ of absolute value \sqrt{q} . Therefore $L(t) = q^g t^{2g} + b_{2g-1} t^{2g-1} + \dots + b_1 t + 1 \in \mathbb{Z}[t]$ is determined by the coefficients b_1, \dots, b_g which are in turn determined by the numbers a_1, \dots, a_g . See for example [Sti, Section 5.1] for more details.

To a genus g curve X having $L(t)$ as numerator of its Zeta function, we associate the so-called *real Weil polynomial* of X :

$$h(t) = \prod_{i=1}^g (t - \mu_i) \in \mathbb{Z}[t],$$

where $\mu_i = \alpha_i + \overline{\alpha_i}$ is a real number in the interval $[-2\sqrt{q}, 2\sqrt{q}]$, for all $i = 1, \dots, g$. We have

$$L(t) = t^g h(qt + 1/t). \quad (1)$$

One can hence turn the problem of determining the Zeta function of X into the problem of determining the real Weil polynomial of X . Not every polynomial $h(t)$ with all zeros in the interval $[-2\sqrt{q}, 2\sqrt{q}]$ and with the property that

$$\frac{L(t)}{(1-t)(1-qt)} = \prod_{d \geq 1} \frac{1}{(1-t^d)^{a_d}}$$

for certain integers $a_d \geq 0$ is necessarily the real Weil polynomial of a curve. The following result is due to Serre [S, page Se 11], [L, Lemma 1].

Proposition 2.1. *Let $h(t)$ be the real Weil polynomial of a curve C over \mathbb{F}_q . Then $h(t)$ cannot be factored as $h(t) = h_1(t)h_2(t)$, with $h_1(t)$ and $h_2(t)$ non-constant polynomials in $\mathbb{Z}[t]$ such that the resultant of $h_1(t)$ and $h_2(t)$ is ± 1 .*

This result has been generalized by E. Howe and K. Lauter. Proposition 2.2 below is an improvement [H] of [H-L, Theorem 1.b)] and Proposition 2.3 is [H-L, Theorem 1, Proposition 13]. Recall that the *reduced resultant* of two polynomials $f, g \in \mathbb{Z}[t]$ is defined to be the non-negative generator of the ideal $(f, g) \cap \mathbb{Z}$.

Proposition 2.2. *Let $h(t) = h_1(t)h_2(t)$ be the real Weil polynomial of a curve C over \mathbb{F}_q , where $h_1(t)$ and $h_2(t)$ are coprime non-constant factors in $\mathbb{Z}[t]$. Let r be the reduced resultant of the radical of $h_1(t)$ and the radical of $h_2(t)$. If $r = 2$, then, there exists a degree 2 map $C \rightarrow C'$, where the curve C' is defined over \mathbb{F}_q and has either $h_1(t)$ or $h_2(t)$ as real Weil polynomial.*

Proposition 2.3. *Let $h(t) = (t - \mu)h_2(t)$ be the real Weil polynomial of a curve C over \mathbb{F}_q , where $t - \mu$ is the real Weil polynomial of an elliptic curve E and $h_2(t)$ a non-constant polynomial in $\mathbb{Z}[t]$ coprime with $t - \mu$. If $r \neq \pm 1$ is the resultant of $t - \mu$ and the radical of $h_2(t)$, then C admits a map of degree dividing r to an elliptic curve isogenous to E .*

For a curve X we denote by $a(X)$ the vector $[a_1, a_2, \dots]$. The main result of this section is the following.

Theorem 2.4. *For $g \leq 6$ the real Weil polynomial $h(t)$ and the vector $a(X)$ of an optimal genus g curve X over \mathbb{F}_2 are as follows:*

$$\begin{aligned} g = 1 : h(t) &= t + 2, & a(X) &= [5, 0, 0, 5, 4, 10, \dots]; \\ g = 2 : h(t) &= t^2 + 3t + 1, & a(X) &= [6, 0, 1, 1, 6, 12, \dots]; \\ g = 3 : h(t) &= t^3 + 4t^2 + 3t - 1, & a(X) &= [7, 0, 1, 0, 7, 7, \dots]; \\ g = 4 : h(t) &= (t + 1)(t + 2)(t^2 + 2t - 2), & a(X) &= [8, 0, 0, 2, 4, 8, \dots]; \\ g = 5 : h(t) &= t(t + 2)^2(t^2 + 2t - 2), & a(X) &= [9, 0, 0, 2, 0, 12, \dots]; \\ g = 6 : & & & \\ & h(t) = t(t + 2)(t^4 + 5t^3 + 5t^2 - 5t - 5), & a(X) &= [10, 0, 0, 0, 3, 10, \dots], \quad (2) \\ & h(t) = (t - 1)(t + 2)(t^2 + 3t + 1)^2, & a(X) &= [10, 0, 0, 0, 2, 15, \dots]. \quad (3) \end{aligned}$$

Proof. Following [S, page Se Th 38] we compute for each $g \leq 6$ a finite list of monic degree g polynomials $h(t) \in \mathbb{Z}[t]$ for which a_1 is equal to the number of \mathbb{F}_2 -rational points of an optimal genus g curve and for which $a_d \geq 0$ for $d \geq 2$ in the relation $L(t) = t^g h(qt + 1/t)$. Moreover we require that $h(t)$ has the property that its zeros are in the interval $[-2\sqrt{2}, 2\sqrt{2}]$. Finally, we require that the conditions of Proposition 2.1 are satisfied. A short computer calculation gives a unique polynomial for $g \leq 5$ and three polynomials for $g = 6$:

- (1) $h(t) = t(t+2)(t^4 + 5t^3 + 5t^2 - 5t - 5), \quad a(X) = [10, 0, 0, 0, 3, 10, \dots];$
- (2) $h(t) = (t-1)(t+2)(t^2 + 3t + 1)^2, \quad a(X) = [10, 0, 0, 0, 2, 15, \dots];$
- (3) $h(t) = (t+1)(t+2)(t^2 + 2t - 2)(t^2 + 2t - 1), \quad a(X) = [10, 0, 0, 1, 0, 12, \dots].$

We show that the third polynomial cannot occur. The resultant of the factors $t + 2$ and $(t + 1)(t^2 + 2t - 2)(t^2 + 2t - 1)$ is -2 . Hence, by Proposition 2.3, a genus $g = 6$ curve X , having this polynomial as real Weil polynomial, admits a degree 2 map $X \rightarrow E$, where E is a genus one curve having real Weil polynomial $t + 2$. The curve E has parameters $a(E) = [5, 0, 0, 5, 4, 10, \dots]$, hence E has five places of degree 4 while X has only one. Since E does not have any degree 2 places, this means that one place Q of the degree 4 places of E must ramify in X . The different D of the quadratic function field extension $\mathbb{F}_2(X)/\mathbb{F}_2(E)$ satisfies $2Q \leq D$ (where the coefficient 2 is forced by wild ramification). On the other hand the degree of the different is $2g - 2 = 10 = \deg D$ by the Hurwitz formula. Thus $D = 2Q + 2R$, where R is a rational point of E . But this is a contradiction because all of five rational points of E split completely in X since $\#X(\mathbb{F}_2) = 10$. \square

3 Uniqueness of optimal elliptic curves

In this section we prove Theorem 1.1 for curves of genus 0 and 1.

Remark 3.1. We denote by \mathbb{P}^1 the projective line over \mathbb{F}_2 and by 0, 1 and ∞ its three rational points. Over a finite field, every genus 0 curve is isomorphic to \mathbb{P}^1 . Therefore \mathbb{P}^1 is optimal. The Zeta function of \mathbb{P}^1 is

$$Z(t) = \frac{1}{(1-2t)(1-t)} \quad \text{and hence} \quad a(\mathbb{P}^1) = [3, 1, 2, 3, 6, \dots].$$

Proposition 3.2. Up to \mathbb{F}_2 -isomorphism, the unique genus 1 curve having five rational points over \mathbb{F}_2 is the elliptic curve E of affine equation $y^2 + y = x^3 + x$.

Proof. A genus 1 curve E over \mathbb{F}_2 having five rational points over \mathbb{F}_2 is an elliptic curve. Hence E admits a separable degree 2 morphism to \mathbb{P}^1 . It can be described as a smooth cubic in \mathbb{P}^2 of affine equation of the form $y^2 + a(x)y = f(x)$, where $a(x)$ and $f(x)$ are polynomials in $\mathbb{F}_2[x]$, the first of degree 0 or 1 and the latter of degree 3 [Sil, Appendix A]. Since the point at infinity ∞ of \mathbb{P}^1 ramifies in E , one has $a(x) = 1$. The affine points 0 and 1 of \mathbb{P}^1 have to split, thus we have that $f(0) = f(1) = 0$ and hence $f(x) = x(x+1)(x+a)$, where $a \in \mathbb{F}_2$. If $a = 1$ we find the equation $y^2 + y = x^3 + x$ and if $a = 0$ the equation $y^2 + y = x^3 + x^2$. These two curves are indeed isomorphic over \mathbb{F}_2 by changing coordinates through the map $(x, y) \mapsto (x+1, y)$. \square

Remark 3.3. The function field of the genus 1 curve E can also be described as the ray class field of \mathbb{P}^1 of conductor 4 times a rational point, in which the other two rational points of \mathbb{P}^1 are both split. Since $\text{Aut}(\mathbb{P}^1)$ acts doubly transitively on $\{0, 1, \infty\}$, different choices give rise to isomorphic ray class fields.

Remark 3.4. We often refer to this unique optimal elliptic curve E throughout this paper. For future reference, we present here some properties of E . In terms of the affine equation $y^2 + y = x^3 + x$, we denote the five rational points of E as follows: we write P_0 for the point at infinity and we put

$$P_1 = (0, 0), \quad P_2 = (0, 1), \quad P_3 = (1, 0), \quad P_4 = (1, 1). \quad (4)$$

The real Weil polynomial of E is $h(t) = t + 2$. The vector $a(E)$ of the numbers a_d of places of degree $d = 1, 2, \dots$ of E is given by

$$a(E) = [5, 0, 0, 5, 4, 10, 20, \dots].$$

Let $a \in \mathbb{F}_{16}$ be a root of $x^4 + x + 1$. Then, the five places of degree 4 of E have coordinates

$$\begin{aligned} Q_1 &= (a^3, a^3 + a), \quad Q_2 = (a^3, a^3 + a + 1), \\ Q_3 &= (a^3 + 1, a), \quad Q_4 = (a^3 + 1, a + 1), \quad Q_5 = (a^2 + a + 1, a). \end{aligned}$$

Let $b \in \mathbb{F}_{32}$ be a root of $x^5 + x^3 + 1$, then the four places of degree 5 of E consist of the points of coordinates:

$$R_1 = (b, b^4), \quad R_2 = (b, b^4 + 1), \quad R_3 = (b + 1, b^4 + b), \quad R_4 = (b + 1, b^4 + b + 1).$$

Let $c \in \mathbb{F}_{64}$ be a root of $x^6 + x^5 + 1 = 0$. The places of degree 6 of E have coordinates

$$\begin{aligned} T_1 &= (c^5 + c^3 + c^2 + c + 1, c^5 + c^4 + c^3 + 1), \quad T_2 = (c^5 + c^3 + c^2 + c, c^4 + c^2 + c), \\ T_3 &= (c^3 + c^2 + 1, c^3 + c^2 + c), \quad T_4 = (c^3 + c^2 + 1, c^3 + c^2 + c + 1), \\ T_5 &= (c + 1, c^4 + c^3 + c^2 + c), \quad T_6 = (c + 1, c^4 + c^3 + c^2 + c + 1), \\ T_7 &= (c^3 + c^2, c + 1), \quad T_8 = (c^3 + c^2, c), \\ T_9 &= (c, c^4 + c^3 + c^2), \quad T_{10} = (c, c^4 + c^3 + c^2 + 1). \end{aligned}$$

The order 5 automorphism σ of E given by addition of P_1 acts transitively on $E(\mathbb{F}_2)$ as follows: $P_0 \mapsto P_1 \mapsto P_3 \mapsto P_4 \mapsto P_2 \mapsto P_0$. The action of σ on the places of degree 4 is as follows: $Q_1 \mapsto Q_5 \mapsto Q_2 \mapsto Q_4 \mapsto Q_3 \mapsto Q_1$. On the other hand, the order 4 automorphism of E

$$\tau : (x, y) \mapsto (x + 1, y + x + 1)$$

fixes P_0 and acts transitively on the remaining four rational points: $P_1 \mapsto P_4 \mapsto P_2 \mapsto P_3 \mapsto P_1$. Similarly, τ fixes Q_5 and acts transitively on the remaining degree 4 places: $Q_1 \mapsto Q_4 \mapsto Q_2 \mapsto Q_3 \mapsto Q_1$. The action of τ on the places of degree 5 is transitive: $R_1 \mapsto R_4 \mapsto R_2 \mapsto R_3 \mapsto R_1$.

4 Uniqueness of genus 2 optimal curves

Proof of Theorem 1.1 for $g = 2$. A genus 2 optimal curve X over \mathbb{F}_2 is hyperelliptic. Since X has six rational points, all three rational points of \mathbb{P}^1 split completely in the double covering $X \rightarrow \mathbb{P}^1$. By Theorem 2.4, the curve X has no places of degree 2 and only one place of degree 3. Thus only one degree 3 place Q of the two degree 3 places of \mathbb{P}^1 totally ramifies in X . The different D of the corresponding function field extension is hence $2Q$, since $2Q \leq D$ and $\deg D = 6$ by the Hurwitz formula. Any genus 2 curve having six rational points over \mathbb{F}_2 is hence a double covering of \mathbb{P}^1 of conductor $2Q$, where Q is a place of \mathbb{P}^1 of degree 3, in which all rational points of \mathbb{P}^1 are split. A different choice of the degree 3 place of \mathbb{P}^1 leads to an \mathbb{F}_2 -isomorphic curve. Indeed, the \mathbb{F}_2 -isomorphism $x \mapsto 1/x$ preserves the rational points of \mathbb{P}^1 , but switches the two degree 3 places. \square

5 Uniqueness of genus 3 optimal curves

We briefly recall some important results on the Jacobian variety of a curve in order to state and prove a useful lemma.

Let X be a curve defined over \mathbb{F}_q . We denote by $\mathcal{J}ac(X)$ the Jacobian variety of X and by T_ℓ the Tate module attached to $\mathcal{J}ac(X)$, where ℓ is a prime number different from the characteristic of \mathbb{F}_q . We set $V_\ell = T_\ell \otimes \mathbb{Q}_\ell$. Let $F : V_\ell \rightarrow V_\ell$ be the Frobenius map and let $V : V_\ell \rightarrow V_\ell$ be the Verschiebung map: the unique map such that $V \circ F = q$. Then $\mathbb{Z}[F, V] \subseteq \text{End}(\mathcal{J}ac(X))$. Next we let ϕ be the canonical polarization on $\mathcal{J}ac(X)$. Then ϕ can be represented as a non-degenerate alternating form $\phi : V_\ell \times V_\ell \rightarrow \mathbb{Q}_\ell$. Here \mathbb{Q}_ℓ denotes the field of ℓ -adic numbers. Since $\phi(F(x), F(y)) = q\phi(x, y)$ for every $x, y \in V_\ell$, by bilinearity of ϕ we have that $\phi(F(x), F(y)) = q\phi(x, y) = \phi(qx, y) = \phi(V(F(x)), y)$. It follows that $\phi(z, F(y)) = \phi(V(z), y)$ for any $y, z \in V_\ell$. In other words V is left adjoint to F with respect to ϕ .

Theorem 5.1 (Torelli Theorem [W]). *Let X and X' be two curves over a perfect field k . Let $\tau : \mathcal{J}ac(X) \rightarrow \mathcal{J}ac(X')$ be an isomorphism over k compatible with the canonical polarizations. Then*

1. *if X is hyperelliptic, there exists a unique isomorphism $f : X \rightarrow X'$ over k which gives τ ;*
2. *if X is not hyperelliptic, there exists a unique isomorphism $f : X \rightarrow X'$ over k and a unique $\varepsilon \in \{\pm 1\}$ such that f gives $\varepsilon\tau$.*

Corollary 5.2. *If τ is an automorphism of $\mathcal{J}ac(X)$ over k preserving the polarization, then either τ or $-\tau$ comes from an automorphism over k of X .*

Lemma 5.3. *Any genus 3 curve X having exactly seven rational points over \mathbb{F}_2 admits an automorphism of order 7.*

Proof. We show that for a genus 3 curve X having seven rational points over \mathbb{F}_2 the ring $\mathbb{Z}[F, V] \subseteq \text{End}(\mathcal{J}ac(X))$ is isomorphic to $\mathbb{Z}[\zeta_7]$, the ring of integers of $\mathbb{Q}(\zeta_7)$. The

minimal polynomial of $F + V$ is the real Weil polynomial of X . By Theorem 2.4 this is $h(t) = t^3 + 4t^2 + 3t - 1$. It is an irreducible polynomial of discriminant 7^2 . Hence, for a root $\alpha \in \overline{\mathbb{Q}}$ of $h(t)$, the number field $\mathbb{Q}(\alpha)$ is a cyclic extension of degree 3 of \mathbb{Q} , which is ramified only at 7. By the Kronecker-Weber Theorem the field $\mathbb{Q}(\alpha)$ is hence the unique degree 3 subfield $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ of $\mathbb{Q}(\zeta_7)$ and $\mathbb{Z}[\alpha]$ is its ring of integers. Consider now the minimal polynomial of Frobenius $x^2 - \alpha x + 2 \in \mathbb{Z}[\alpha][x]$. Its discriminant $\alpha^2 - 8$ has norm 7 and hence generates a prime ideal $\pi \subseteq \mathbb{Z}[\alpha]$ lying over the prime 7 of \mathbb{Z} . By class field theory $\mathbb{Q}(\alpha)$ admits a unique quadratic extension unramified outside of π and the three infinite primes lying over 7. This is the field $\mathbb{Q}(\zeta_7)$, which has discriminant 7^5 by the conductor-discriminant formula. The discriminant of $\mathbb{Q}(\alpha, x)$ can be computed to be 7^5 as well by means of the relative discriminant formula for towers of number fields. Hence $\mathbb{Z}[F, V] = \mathbb{Z}[\alpha, x]$ is the ring of integers $\mathbb{Z}[\zeta_7]$ of $\mathbb{Q}(\zeta_7)$ as wanted.

Now $\mathcal{I}ac(X)$ has in particular an automorphism τ of order 7 corresponding to ζ_7 . We show that τ preserves the polarization ϕ . By bilinearity of ϕ and since V is the complex conjugate of F , the left adjoint to an element $\tau \in \mathbb{Z}[F, V]$ is its complex conjugate $\bar{\tau}$. Since τ satisfies $\tau\bar{\tau} = 1$, we have in particular that $\phi(\tau(x), y) = \phi(x, \bar{\tau}(y)) = \phi(x, \tau^{-1}(y))$ for any x, y in V_ℓ . This implies that $\phi(\tau(x), \tau(y)) = \phi(x, y)$ for any $x, y \in V_\ell$. In other words τ preserves the polarization ϕ of $\mathcal{I}ac(X)$. By the above Corollary of Torelli's Theorem the curve X admits hence an automorphism f of order 7. Indeed if f does not induce τ of order 7, but f induces $-\tau$, then f^2 is an automorphism of order 7 of X . \square

Proof of Theorem 1.1 for $g = 3$. By Lemma 5.3 the curve X admits an automorphism f of order 7. Then, by Galois correspondence, X is a cyclic covering of degree 7 of a curve which can only be \mathbb{P}^1 by comparing the genera and the degree of the different in the Hurwitz formula. By the conductor-discriminant formula, the conductor D of such a covering satisfies $6 \deg D = 18$. Since there are seven rational points on X , only one rational point P of \mathbb{P}^1 splits completely. Thus one has $D = Q$, where Q is a place of \mathbb{P}^1 of degree 3. Hence X is a cyclic degree 7 covering of \mathbb{P}^1 of conductor Q , where one rational point P of \mathbb{P}^1 splits completely. Different choices of P in $\{0, 1, \infty\}$ and of the degree 3 place Q give rise to \mathbb{F}_2 -isomorphic curves. Indeed, since the automorphisms group of \mathbb{P}^1 acts transitively on the rational points, we can always first reduce to the case $P = \infty$. Next the automorphism $x \mapsto x + 1$ fixes P and maps one degree 3 place of \mathbb{P}^1 into the other one. \square

6 Uniqueness of genus 4 optimal curves

Proof of Theorem 1.1 for $g = 4$. By Theorem 2.4 the real Weil polynomial of an optimal genus 4 curve X over \mathbb{F}_2 is $h(t) = (t+1)(t+2)(t^2+2t-2)$. The resultant of the polynomials $t+2$ and $(t+1)(t^2+2t-2)$ is 2. Proposition 2.3 implies therefore that the curve X is a double covering of the unique optimal elliptic curve E having real Weil polynomial $t+2$ described in Remark 3.4. Since X has no places of degree 2, no rational point of E can be inert in X . Hence, since X has eight rational points, there is only one possibility for the five rational points of E : three of them split completely

and two are totally ramified. Denoting by P and P' the two wildly ramified rational points of E , we have that the contribution to the different of the quadratic function field extension $\mathbb{F}_2(X)/\mathbb{F}_2(E)$ is at least $2P + 2P'$. Since the degree of the different has to be 6 by the Hurwitz formula, the different, which is also the conductor of the extension, is $4P + 2P'$ or $2P + 4P'$. Thus any optimal genus 4 curve over \mathbb{F}_2 is a double covering of the optimal elliptic curve E of conductor $4P + 2P'$ or $2P + 4P'$, in which the other three rational points of E split completely. Uniqueness of X follows from the fact that $\text{Aut}(E)$ acts doubly transitively on $E(\mathbb{F}_2)$ as described in Remark 3.4. \square

7 Uniqueness of genus 5 optimal curves

Lemma 7.1. *Let C be the hyperelliptic curve over \mathbb{F}_2 of affine equation $y^2 + y = x^5 + x^3$. Let P be a rational point of C and let K be the ray class field of $\mathbb{F}_2(C)$ of conductor $4P$ in which all rational points of C except P split completely. Then $K = \mathbb{F}_2(C)$ except when P is the point at infinity, in which case we have $[K : \mathbb{F}_2(C)] = 2$.*

Proof. Let t denote a uniformizer at P and let $S = C(\mathbb{F}_2) \setminus \{P\}$. By Artin reciprocity the Galois group $\text{Gal}(K/\mathbb{F}_2(C))$ is isomorphic to the S -ray class group of C modulo $4P$ [N-X, Section 2.5]. In this case the latter is isomorphic to a quotient of $R = \left(\mathbb{F}_2[[t]]/(t^4)\right)^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ by the S -unit group of C [Sch, Section 8]. We show that if P is the point at infinity of C we have $\text{Gal}(K/\mathbb{F}_2(C)) \simeq \mathbb{Z}_2$. On the other hand, if P is one of the other rational points

$$P_0 = (0, 0), P'_0 = (0, 1), P_1 = (1, 0), \text{ or } P'_1 = (1, 1)$$

of C , the group $\text{Gal}(K/\mathbb{F}_2(C))$ is trivial. A sketch of the computations follows.

- i) Let P be the point at infinity of C . Then a basis for the S -unit group of C consists of the functions with principal divisors given by

$$\begin{aligned} \left(\frac{y+x^3}{x^3}\right) &= 2P_0 + P'_1 - 3P'_0, \\ \left(\frac{y+1}{y}\right) &= 3(P'_0 - P_0) + 2(P'_1 - P_1), \\ \left(\frac{x+1}{x}\right) &= P_1 - P_0 + P'_1 - P'_0. \end{aligned}$$

Let $t = y/x^3$ be a uniformizer at P , then their images in R are:

$$\begin{aligned} \frac{y+x^3}{x^3} &\equiv 1+t \pmod{t^4}, \\ \frac{y+1}{y} &= 1 + \frac{1}{y} \equiv 1+t^5 \equiv 1 \pmod{t^4}, \\ \frac{x+1}{x} &= 1 + \frac{1}{x} \equiv 1+t^2 \pmod{t^4}, \end{aligned}$$

since $1/y = t^5 + O(t^6)$ and $1/x = t^2 + O(t^4)$. The element $1 + t$ generates a subgroup R' of R of index 2 and $1 + t^2 \in R'$. Therefore $\text{Gal}(K/\mathbb{F}_2(C)) \simeq R/R' \simeq \mathbb{Z}_2$.

ii) Let $P = P_0$ and x a uniformizer at P . In this case consider the two \mathbb{F}_2 -linearly independent S -units of divisors given by

$$\begin{aligned}(x+1) &= P_1 + P'_1 - 2P_\infty, \\ (y+1) &= 3P'_0 + 2P'_1 - 5P_\infty.\end{aligned}$$

Here P_∞ denotes the point at infinity of C . By means of Hensel's lemma, we compute the local expansion of y at P_0 as $y = x^5 + x^3 + O(x^6)$. Therefore their images in R are

$$\begin{aligned}x+1 &\equiv 1+x \pmod{x^4}, \\ y+1 &\equiv 1+x^3 \pmod{x^4}.\end{aligned}$$

In this case the group R is generated by the images of the S -units and thus the quotient group is trivial.

The other possibilities for P reduce to case ii) by applying the order 4 automorphism $\varphi : (x, y) \mapsto (x+1, y+x^2+1)$ of C . It fixes the point at infinity of C and acts transitively on the other rational points of C . \square

Proof of Theorem 1.1 for $g = 5$. By Theorem 2.4 a genus 5 optimal curve X defined over \mathbb{F}_2 has real Weil polynomial $h(t) = t(t+2)^2(t^2+2t-2)$. Since the principal ideal $(t(t+2), t^2+2t-2) \cap \mathbb{Z}$ is generated by 2, Proposition 2.2 implies that the curve X is a double covering of a curve C having real Weil polynomial either $t(t+2)^2$ or t^2+2t-2 . If C had $t(t+2)^2$ as real Weil polynomial, it would be a genus 3 curve having seven rational points over \mathbb{F}_2 , which is impossible by Theorem 2.4.

Hence C is a genus 2 curve having five rational points and no place of degree 2. Every genus 2 curve defined over \mathbb{F}_2 is a hyperelliptic curve. Up to \mathbb{F}_2 -isomorphism there exists a unique hyperelliptic curve C over \mathbb{F}_2 having real Weil polynomial t^2+2t-2 . Indeed such a hyperelliptic curve has five rational points and no place of degree 2. Thus the different of the function field extension associated to the double covering $C \rightarrow \mathbb{P}^1$ has to be $6Q$, where Q is a rational point of \mathbb{P}^1 . According to the classification of genus 2 curves over \mathbb{F}_2 in [M-N, page 327], by taking $Q = \infty$, any such hyperelliptic curve is \mathbb{F}_2 -isomorphic to a projective curve of affine equation $y^2+y = x^5+ax^3+bx^2+c$, with $a, b, c \in \mathbb{F}_2$. Of the eight possible equations arising from the choice of the parameters a, b, c , only the affine equation $y^2+y = x^5+x^3$ describes a projective curve having five rational points over \mathbb{F}_2 and no places of degree 2.

Since X has nine rational points, only one rational point P of C ramifies in the double covering $X \rightarrow C$, while the other four rational points of C split completely in X . The different of $\mathbb{F}_2(X)/\mathbb{F}_2(C)$ is hence $4P$, since it must have degree 4 by the Hurwitz formula. The function field $\mathbb{F}_2(X)$ is hence an abelian extension of $\mathbb{F}_2(C)$ of conductor $4P$, where the other four rational points of C split completely. The maximal among such abelian extensions is the ray class field K described in Lemma 7.1. Hence P is the point at infinity of C and $\mathbb{F}_2(X) = K$. \square

8 Genus $g = 6$ optimal curves

Theorem 2.4 lists the two possible real Weil polynomials of an optimal genus 6 curve defined over \mathbb{F}_2 . In this section we give a proof of the existence of a unique genus 6 curve for each of the two listed polynomials.

Proposition 8.1. *Up to \mathbb{F}_2 -isomorphism, there is a unique curve having real Weil polynomial as in (2) of Theorem 2.4.*

Proof. Let X be a genus 6 optimal curve defined over \mathbb{F}_2 having real Weil polynomial $h(t) = t(t+2)(t^4 + 5t^3 + 5t^2 - 5t - 5)$. Since the resultant of the factors $t+2$ and $t(t^4 + 5t^3 + 5t^2 - 5t - 5)$ is -2 , there exists a degree 2 morphism $X \rightarrow E$ by Proposition 2.3. All of the five rational points of E split completely into the ten rational points of X . By the Hurwitz formula the degree of the different of $\mathbb{F}_2(X)/\mathbb{F}_2(E)$ is 10. Now, since $a_2(X) = a_3(X) = a_4(X) = 0$, the different is precisely $2R$, where R is a degree 5 place of E . Thus, any such optimal genus 6 curve is a double covering of E of conductor $2R$, in which all rational points of E are split. As observed in Remark 3.4, the elliptic curve E has actually four points of degree 5 and the \mathbb{F}_2 -automorphism τ of E acts transitively on them. The choice of a different degree 5 ramifying point, gives thus an \mathbb{F}_2 -isomorphic curve. \square

In the rest of the section, let X be a genus 6 optimal curve over \mathbb{F}_2 having real Weil polynomial as in (3) of Theorem 2.4.

Proposition 8.2. *Up to \mathbb{F}_2 -isomorphism, there is a unique curve having real Weil polynomial as in (3) of Theorem 2.4.*

Lemma 8.3. *The curve X is a non-Galois covering of degree 3 of the elliptic curve E such that X is unramified outside of $E(\mathbb{F}_2)$.*

The following definition introduces a notation for the splitting behavior of the rational points of the elliptic curve E .

Definition 8.4. *Let $X \rightarrow E$ be a degree 3 covering defined over \mathbb{F}_2 . Consider a rational point P of E . We say that P is*

- a) *an A-point, if P splits completely in X ;*
- b) *a B-point, if P splits into two points of X , one unramified and the other one with ramification index 2;*
- c) *a C-point, if P is totally ramified in X with ramification index 3.*

Moreover we denote by a, b, c the number of A-points, B-points and C-points of E respectively.

Proof of Lemma 8.3. By Theorem 2.4, the real Weil polynomial of X is $h(t) = (t-1)(t+2)(t^2+3t+1)^2$. Since the resultant of the polynomials $t+2$ and $(t-1)(t^2+3t+1)$ is equal to 3, by Proposition 2.3 the curve X admits a morphism of degree 3 to the optimal elliptic curve E described in Remark 3.4. Since the parameters of X are

$a(X) = [10, 0, 0, 0, 2, 15, \dots]$, there are no places of degree 2 or 3 on X . Therefore each of the \mathbb{F}_2 -rational points in E can hence be either an A -point, a B -point or a C -point in the sense of Definition 8.4. Then we have

$$a + b + c = 5 \quad \text{and} \quad 3a + 2b + c = 10,$$

and hence

$$2a + b = 5 \quad \text{and} \quad a = c.$$

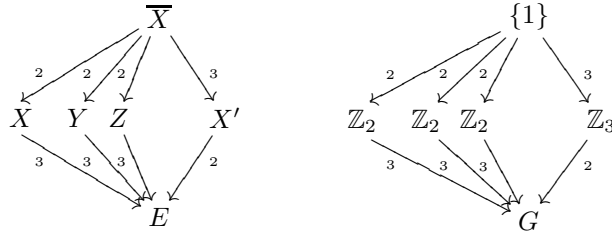
This leaves us with the three cases of Table 1. In each case the covering $X \rightarrow E$ is

	a	b	c
case I	0	5	0
case II	1	3	1
case III	2	1	2

Table 1: Splitting behavior of the rational points of E in X

non-Galois since b is never zero. Moreover the function field extension $\mathbb{F}_2(X)/\mathbb{F}_2(E)$ is unramified outside of $E(\mathbb{F}_2)$. Consider indeed the degree of the different, which is 10 by the Hurwitz formula. By Definition 8.4, only one of the two points of X lying over a B -point of E is wildly ramified. This gives a contribution to the degree of the different which is at least 2. The contribution to the different that comes from the rational points of E is therefore at least $db + 2c$ with $d \geq 2$. Therefore it is at least $5 \cdot 2 = 10$ in case I, at least $3 \cdot 2 + 2 = 8$ in case II and at least $1 \cdot 2 + 2 \cdot 2 = 6$ in case III. Since there are no points of degree 2, 3 or 4 on X , any other non-rational ramified place of E should have degree strictly larger than 4. But this would give a too large contribution to the different in each of the three cases. Hence there are no other places of E ramifying in X but those of degree one. \square

Definition 8.5. We denote by \overline{X} the curve whose function field is the normal closure of $\mathbb{F}_2(X)$ with respect to $\mathbb{F}_2(E)$: it is a Galois extension of $\mathbb{F}_2(E)$ having Galois group isomorphic to the symmetric group S_3 . We denote by X' the curve having as function field the quadratic extension of $\mathbb{F}_2(E)$ corresponding to the group $A_3 \simeq \mathbb{Z}_3$, the unique (normal) subgroup of S_3 of index 2. The situation is described in the following picture:



We sum up some arithmetical properties of X' and \overline{X} in the following auxiliary lemmas.

Lemma 8.6.

- a) The A -points of E split completely in \overline{X} and X' .
- b) Over each B -point of E there are three points of \overline{X} , each with ramification index 2 and there is one point of X' with ramification index 2.
- c) Over each C -point of E there is a unique place of \overline{X} of degree 2.

Proof. Let Y be the degree 3 covering of E as in the picture above.

- a) Each A -point P of E splits completely over $\mathbb{F}_2(Y) \simeq \mathbb{F}_2(X)$ as well. Hence the function field of \overline{X} , being the compositum of $\mathbb{F}_2(X)$ and $\mathbb{F}_2(Y)$, is the splitting field of P . Moreover, since the function field of X' is contained in it, P splits completely in X' as well.
- b) Since there is more than one point of \overline{X} lying over a B -point P of E , the decomposition groups of the points lying over P have order 2. Since the ramification index of one of the points of X lying over P is 2, all points of \overline{X} lying over P have ramification 2. It also follows that there is a unique point of X' lying over P . It has ramification index 2.
- c) Let P be a C -point of E . Since the order of the inertia group of any of the points of \overline{X} lying over P has order divisible by 3, the same is true for a point P' of X' lying over P . It follows that $\overline{X} \rightarrow X'$ is a cyclic degree 3 covering that is ramified at P' . Therefore, by class field theory, the multiplicative group of the residue field of P' must have order divisible by 3. It follows that P must be inert in X' . Indeed, in this case the residue field of P' is \mathbb{F}_4 . \square

Lemma 8.7. *The curve X' is defined over \mathbb{F}_2 and has genus $g' = 6 - c$. Moreover, the covering $X' \rightarrow E$ is ramified exactly at the B -points of E .*

Proof. Since $X \rightarrow E$ is unramified outside of $E(\mathbb{F}_2)$ by Lemma 8.3, the same holds for the covers \overline{X} and X' of E . Lemma 8.6 implies then that $X' \rightarrow E$ is ramified precisely at the B -points of E . By Table 1 there is always at least one such point. Thus, since the residue field of any place contains the constant field, the constant field of X' is \mathbb{F}_2 . In order to compute the genus of X' we compare the different $\text{Diff}(X'/E)$ of $\mathbb{F}_2(X')/\mathbb{F}_2(E)$ with the different $\text{Diff}(X/E)$ of $\mathbb{F}_2(X)/\mathbb{F}_2(E)$. By the Hurwitz formula we have that $10 = 2 \cdot 6 - 2 = \deg \text{Diff}(X/E) = \deg \text{Diff}(X/E)_{\text{tame}} + \deg \text{Diff}(X/E)_{\text{wild}}$. The contribution given to $\text{Diff}(X/E)$ by the c tamely ramified points is $2c$. Therefore the contribution of the b wildly ramified points is $10 - 2c$. Since these are precisely the points that are ramified in $X' \rightarrow E$, the degree of $\text{Diff}(X'/E)$ is also equal to $10 - 2c$. It follows that $2g' - 2 = 10 - 2c$, so that $g' = 6 - c$ as required. \square

Lemma 8.8. *For low degrees d , the number a_d of places of degree d of the curves \overline{X} and X' are as follows:*

$$\begin{aligned} a_1(\overline{X}) &= 6a + 3b, & a_1(X') &= 2a + b; \\ a_2(\overline{X}) &= c, & a_2(X') &= c; \\ a_3(\overline{X}) &= 0, & a_3(X') &= 0; \\ a_4(\overline{X}) &= 0, & a_4(X') &= 10; \\ a_5(\overline{X}) &= 0. \end{aligned}$$

Proof. The computation of the numbers $a_1(\overline{X})$ and $a_1(X')$ of \mathbb{F}_2 -rational points of \overline{X} and X' respectively, follows directly by Lemma 8.6. By the same Lemma the degree 2 places of X' are precisely the ones lying over the C -points of E and they are themselves totally ramified in \overline{X} . This gives $a_2(X') = c = a_2(\overline{X})$. Because of Theorem 2.4, the curve X has parameters $a(X) = [10, 0, 0, 0, 2, 15, \dots]$ and in particular $a_3(X) = 0$. Since also $a_3(E) = 0$, it follows at once that $a_3(X') = a_3(\overline{X}) = 0$. The curve X has no places of degree 2 or 4, thus $a_4(\overline{X}) = 0$. Moreover this means that the five places of degree 4 of E are inert in X . Since they are not ramified, their decomposition group has to be cyclic and hence of order 3. Therefore they are split in X' and we have

$$a_4(X') = 2a_4(E) = 2 \cdot 5 = 10.$$

Suppose that $a_5(\overline{X})$ is not zero, then one of the places of degree 5 of E splits completely in \overline{X} . This implies that X has at least three places of degree 5, which is not the case. Therefore $a_5(\overline{X}) = 0$. \square

The following Lemma describes abelian extensions K_D of $\mathbb{F}_2(E)$ for particular choices of the conductor D . These extensions play a role in the proof of Proposition 8.10. The divisor D is a sum of points in $E(\mathbb{F}_2)$. See Remark 3.4 for the notation.

Lemma 8.9. *Let K_D denote the ray class field of $\mathbb{F}_2(E)$ of conductor D in which the point at infinity and all places of degree 4 of E split completely. Then K_D is trivial when $D = 4P_1 + 2P_2 + 2P_3$ or $D = 2P_1 + 2P_2 + 4P_3$. It has degree 2 over $\mathbb{F}_2(E)$ when $D = 2P_1 + 4P_2 + 2P_3$.*

Proof. Let Q_1, Q_2, \dots, Q_5 denote the degree 4 places of E as listed in Remark 3.4 and let $S = \{Q_1, Q_2, Q_3, Q_4, Q_5, P_0\}$. A basis for the S -unit group of E is given by the following functions u_i , $i = 1, \dots, 5$:

$$\begin{aligned} u_1 &= x^4 + x^3 + x^2 + x + 1, & \text{with } (u_1) &= Q_1 + Q_2 - 8P_0, \\ u_2 &= x^4 + x^3 + 1, & \text{with } (u_2) &= Q_3 + Q_4 - 8P_0, \\ u_3 &= x^2 + x + 1, & \text{with } (u_3) &= Q_5 - 4P_0, \\ u_4 &= \frac{(y + x^3)(y + x^3 + x^2)^2}{y(y + x)(x^2 + x + 1)^3}, & \text{with } (u_4) &= Q_1 + 2Q_3 - 3Q_5, \\ u_5 &= \frac{(y + x^3)^2(y + x^3 + x^2 + 1)}{(y + 1)(y + x)(x^2 + x + 1)^3}, & \text{with } (u_5) &= Q_4 + 2Q_1 - 3Q_5. \end{aligned}$$

Then consider the ray class field $K_{D'}$ of $\mathbb{F}_2(E)$ of conductor $D' = 4P_1 + 4P_2 + 4P_3$ in which the places in S split completely. We are interested in the ray class fields K_{D_j} , $j = 1, 2, 3$, that are subfields of $K_{D'}$ of conductor $D_1 = 4P_1 + 2P_2 + 2P_3$, $D_2 = 2P_1 + 4P_2 + 2P_3$ and $D_3 = 2P_1 + 2P_2 + 4P_3$. The corresponding S -ray class groups modulo D_j are quotients of the groups $R_j = \left(\mathbb{F}_2[[t_j]]/(t_j^4)\right)^* \oplus \left(\mathbb{F}_2[[t_{j'}]]/(t_{j'}^2)\right)^* \oplus \left(\mathbb{F}_2[[t_{j''}]]/(t_{j''}^2)\right)^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ by the image of the S -unit group of E [Sch, Section 8]. Here t_j , $t_{j'}$, $t_{j''}$ denote uniformizers of P_j , $P_{j'}$, $P_{j''}$ respectively, for $\{j, j', j''\} = \{1, 2, 3\}$. We show that the order of the S -ray class group modulo D_j is 2 for $j = 2$, while for $j = 1, 3$ this group is trivial. In Table 2, we display in the column marked by R_j , $j = 1, 2, 3$, the images of the u_i 's ($i \neq 3$) in the group R_j . We remark that the computations for the units u_4 and u_5 can be performed calculating the local expansions y_j of y at P_j , for $j = 1, 2, 3$:

$$\begin{aligned} y_1 &= x + x^2 + x^3 + x^4 + x^6 + O(x^7), \\ y_2 &= 1 + x + x^2 + x^3 + x^4 + x^6 + O(x^7), \\ y_3 &= t^2 + t^3 + t^4 + t^6 + O(t^7), \text{ where } t = x + 1. \end{aligned}$$

u_i	R_1	R_2	R_3
u_1	$(1 + t_1)^3(1 + t_2)$	$(1 + t_1)(1 + t_2)^3$	$(1 + t_1)(1 + t_3^3)(1 + t_2)$
u_2	$(1 + t_1^3)(1 + t_3)$	$(1 + t_2^3)(1 + t_3)$	$(1 + t_3)^3$
u_4	$(1 + t_1)^2(1 + t_1^3)(1 + t_2)$	$(1 + t_2)^3(1 + t_2^3)$	$1 + t_2$
u_5	$1 + t_3$	$(1 + t_2^3)(1 + t_3)$	$(1 + t_3)^3(1 + t_3^3)$

Table 2: Images of the u_i 's in the group R_j , for $j = 1, 2, 3$.

One checks that in R_2 the images of the u_i 's for $i \neq 3$ generate a subgroup of index 2. The image of u_3 is $(1 + t_1)(1 + t_2)^3(1 + t_2^3)(1 + t_3)$ and lies hence in the same subgroup. On the other hand, the images of the u_i 's, $i \neq 3$, are independent generators of R_1 : the image of u_1 has order 4 and the images of u_2 , u_4 and u_5 have order 2. Thus in this case the ray class group is trivial. Similarly for the images of u_1 , u_2 , u_4 and u_5 in R_3 : also in this case the ray class group is trivial. \square

Proposition 8.10. *All rational points of E are ramified in X' . The curve X' has genus 6 and real Weil polynomial $h(t) = t(t + 2)(t^2 - 5)^2$. In other words, only the configuration of case I in Table 1 is possible.*

Proof. According to Table 1, there are three possibilities for the splitting behavior of the rational points of E in X . Moreover by Lemmas 8.7 and 8.8 the genus g' and the vector $a(X')$ of the curve X' are in the three cases as follows:

	a	b	c	g'	$a(X')$
case I	0	5	0	6	$[5, 0, 0, 10, \dots]$
case II	1	3	1	5	$[5, 1, 0, 10, \dots]$
case III	2	1	2	4	$[5, 2, 0, 10, \dots]$

Case *III* cannot occur since in this case the curve X' would be a genus 4 curve having $N_4 = N + 2a_2 + 4a_4 = 5 + 2 \cdot 2 + 4 \cdot 10 = 49$ rational points over \mathbb{F}_{2^4} , while $N_4(4) = 45$ according to [G-V].

In case *II* a computer calculation gives only one possible real Weil polynomial for X' , namely $h(t) = (t+2)(t^2-5)(t^2-2)$. Now, since the automorphism group of E acts doubly transitively on $E(\mathbb{F}_2)$ as described in Remark 3.4, we may assume that the point at infinity P_0 of E is the unique A -point of E and that $P_4 = (1, 1)$ is the unique C -point. The remaining three rational points of E are $\{P_1, P_2, P_3\}$. They are B -points of E and hence ramify in $X' \rightarrow E$ by Lemma 8.6. Moreover, since $a_4(X') = 10$ and $a_4(E) = 5$, all five degree 4 places of E split completely in X' . By the Hurwitz formula the degree of the different of $\mathbb{F}_2(X')/\mathbb{F}_2(E)$ is 8. Therefore Lemma 8.9 implies that $\mathbb{F}_2(X')$ is equal to the ray class field of $\mathbb{F}_2(E)$ of conductor $2P_1 + 4P_2 + 2P_3$, in which P_0 and all degree 4 places of E split completely. Consider now the curve \bar{X} . It is a degree 3 abelian covering of X' . Since \bar{X} has 15 rational points by Lemma 8.8, all five rational points of X' split completely in \bar{X} . Moreover, since $X \rightarrow E$ and $X' \rightarrow E$ are both unramified outside of $E(\mathbb{F}_2)$, only the degree 2 place P'_4 of X' , which lies over P_4 of E ramifies in \bar{X} . The curve \bar{X} is hence the ray class field of $\mathbb{F}_2(X')$ of conductor P'_4 , where all rational places of X' split completely. A computer calculation with MAGMA shows that the associated ray class group is trivial. Hence case *II* cannot occur.

In case *I* a computer calculation gives only one possible real Weil polynomial for X' , namely $h(t) = t(t+2)(t^2-5)^2$. \square

In the next two lemmas we describe two curves appearing in the proof of Proposition 8.2.

Lemma 8.11. *There exists a unique curve C having real Weil polynomial $h(t) = (t+2)(t-1)$. Up to \mathbb{F}_2 -isomorphism, this is a genus 2 projective curve described by the affine equation $y^2 + xy = x^5 + x^4 + x^2 + x$.*

Proof. A curve C having real Weil polynomial $h(t) = (t+2)(t-1)$ is a genus 2 curve having four rational points and two places of degree 2 over \mathbb{F}_2 . Since it is a hyperelliptic curve, we can consider the double covering $C \rightarrow \mathbb{P}^1$. The different of the corresponding function field extension is $4P + 2P'$, where P and P' are rational points of \mathbb{P}^1 . Indeed, by the Hurwitz formula, the degree of the different is 6 and, since C has four rational points, two of the rational points of \mathbb{P}^1 are wildly ramified and one splits completely. The coefficients of P and P' are forced to be even since $\mathbb{F}_2(C)$ is an Artin-Schreier extension of the rational function field. Notice also that the possibility that two rational points of \mathbb{P}^1 split and the third stays inert in $\mathbb{F}_2(C)$ is excluded by the fact that in this case the degree 2 place of \mathbb{P}^1 would be ramified, giving a contradiction in the computation of the different. According to the classification of genus 2 curves over \mathbb{F}_2 in [M-N, page 327], by taking $P = P_\infty$ and $P' = (0, 0)$, any such a hyperelliptic curve over \mathbb{F}_2 is \mathbb{F}_2 -isomorphic to a projective curve of affine equation $y^2 + y = x^3 + ax + 1/x + b$, with $a, b \in \mathbb{F}_2$. There are hence four possibilities for the parameters a and b , but only $y^2 + y = x^3 + x + 1/x + 1$ is the equation of a projective curve having four rational points over \mathbb{F}_2 and two places of degree

2. This curve is \mathbb{F}_2 -isomorphic to the projective curve of more simple affine equation $y^2 + xy = x^5 + x^4 + x^2 + x$, an isomorphism being given by $(x, y) \mapsto (x, (y + x^2)/x)$. \square

Lemma 8.12. *Let C be the curve of Lemma 8.11. Then C admits an unramified cyclic degree 5 covering in which both the point at infinity P_∞ and the point $(0, 0)$ split. This covering is unique up to isomorphism. Moreover, for any other choice of rational points P and P' of C , any cyclic unramified degree 5 covering of C in which P and P' split, is necessarily trivial.*

Proof. Consider the maximal unramified extension L of the function field K of C where P_∞ splits completely. By class field theory, the Galois group $\mathcal{G}al(L/K)$ is isomorphic to the quotient of the class group $Pic(C)$ by the subgroup generated by the image in $Pic(C)$ of the Frobenius element $\text{Frob } P_\infty \in \mathcal{G}al(L/K)$ of P_∞ . Hence $\mathcal{G}al(L/K) \simeq Pic^0(C)$. Let $h(t)$ be the real Weil polynomial of C as in Lemma 8.11. By [Sti, Theorem 5.1.15 (c)] the class number $\#Pic^0(C)$ of C equals $L(1)$, where $L(t)$ is the numerator of the Zeta function of C . Since $L(1) = h(q + 1)$ by (1), one has $\#Pic^0(C) = h(3) = 10$. Therefore there exists a unique unramified cyclic degree 5 extension K' of $\mathbb{F}_2(C)$ in which P_∞ splits completely. Since the divisor $(x) = 2((0, 0) - P_\infty)$ is principal, the Frobenius of $(0, 0)$ is trivial in $\mathcal{G}al(K'/K) \simeq \mathbb{Z}_5 \simeq Pic^0(C)/\mathbb{Z}_2$, so that the rational point $(0, 0)$ is also split in K' .

On the other hand, if we replace the points P_∞ and $(0, 0)$ by any other pair of rational points of C , there is no such unramified cyclic degree 5 extension. To see this, we note that C has four rational points: P_∞ , $(0, 0)$, $(1, 0)$ and $(1, 1)$. If two of these were to split in an unramified cyclic degree 5 covering of C , then 2 times their difference, would be a principal divisor. By adding or subtracting the principal divisors $2((0, 0) - P_\infty)$ and $2((1, 0) + (1, 1) - 2P_\infty)$, this boils in each case down to the question of whether or not the divisor $2((1, 0) - P_\infty)$ is principal. Suppose that $2((1, 0) - P_\infty)$ is the divisor of a function $f \in \mathbb{F}_2(C)$. Since the only functions in $\mathbb{F}_2(C)$ with a pole of order 2 at infinity are linear functions in x , we must have $f = x + 1$, but then f also vanishes in $(1, 1)$, a contradiction. \square

Proof of Proposition 8.2. By Lemma 8.3 the genus 6 curve X is a non-Galois covering of degree 3 of the elliptic curve E . Moreover, by Proposition 8.10 the only possibility for the splitting behavior of the rational points of E in X is described in case I of Table 1. In other words, all rational points of E are B -points in the sense of Definition 8.4. In order to show that such a curve X is unique, consider the quadratic function field extension $\mathbb{F}_2(X')/\mathbb{F}_2(E)$ described in the picture of Definition 8.5. By the Hurwitz formula and Proposition 8.10, this is an abelian extension of $\mathbb{F}_2(E)$ of conductor $\sum_{i=0}^4 2P_i$ where all places of E of degree 4 split completely.

Let τ be the order 4 automorphism of E described in Remark 3.4. Then the endomorphism $\tau + 2$ of the elliptic curve E has degree 5 and kernel $E(\mathbb{F}_2)$. The Galois group of the covering $\tau + 2 : E \rightarrow E$ consists of the translations by the points P_i of E . It preserves both the set $E(\mathbb{F}_2)$ and the set of places of E of degree 4. Therefore the covering

$$X' \longrightarrow E \xrightarrow{\tau+2} E$$

is Galois. Similarly, the covering $\overline{X} \rightarrow X'$ is unramified and cyclic of degree 3. Lemma 8.8 implies that all rational points of X' are split. By class field theory, there exists a unique degree 3 such a covering of X' . Indeed, let $h(t)$ be the real Weil polynomial of X' as in Proposition 8.10. By [Sti, Theorem 5.1.15 (c)] one has $\#Pic^0(X') = L(1)$, where $L(t)$ is the numerator of the Zeta function of X' . Hence, since by (1) one has $L(1) = h(3) = 2^4 \cdot 3 \cdot 5$, there exists a unique index 3 subgroup in the class group of X' . Thus the function field extension corresponding to the covering

$$\overline{X} \longrightarrow E \xrightarrow{\tau+2} E$$

is also Galois. The Galois group G is an extension of \mathbb{Z}_5 by S_3 . Since these groups have coprime order and \mathbb{Z}_5 necessarily acts trivially on S_3 , the Schur-Zassenhaus Theorem implies that G is a direct product of \mathbb{Z}_5 and S_3 . By Galois correspondence there exists hence a tower of function fields corresponding to the morphisms of curves $\overline{X} \rightarrow Y \rightarrow E$, such that $\mathcal{Gal}(\mathbb{F}_2(Y)/\mathbb{F}_2(E)) \simeq S_3$. Let ρ be a generator of $\mathcal{Gal}(\mathbb{F}_2(\overline{X})/\mathbb{F}_2(X)) \subseteq S_3$ and consider invariant fields. We obtain a cyclic covering $X \rightarrow C$ of degree 5, which is unramified since $\tau + 2 : E \rightarrow E$ is.

$$\begin{array}{ccc} Y & \xleftarrow{5} & \overline{X} \\ \downarrow 2 & & \downarrow 2 \\ C & \xleftarrow{5} & X \\ \downarrow 3 & & \downarrow 3 \\ E & \xleftarrow{5} & E \end{array} \quad \begin{array}{ccc} \mathbb{Z}_5 & \xleftarrow{5} & \{1\} \\ \downarrow 2 & & \downarrow 2 \\ \mathbb{Z}_5 \times \mathbb{Z}_2 & \xleftarrow{5} & \mathbb{Z}_2 \\ \downarrow 3 & & \downarrow 3 \\ \mathbb{Z}_5 \times S_3 & \xleftarrow{5} & S_3 \end{array}$$

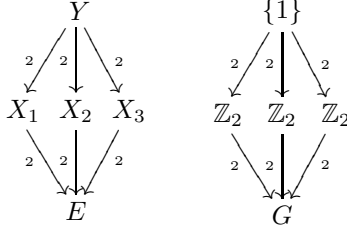
The curve C has genus 2 by the Hurwitz formula. The real Weil polynomial of C is thus a degree 2 factor of the real Weil polynomial of X . Since C is also a degree 3 covering of E , the real Weil polynomial of C is divisible by the real Weil polynomial $t+2$ of E , since the same holds for the corresponding Zeta functions [A-P]. Hence the real Weil polynomial of C is $h(t) = (t+2)(t-1)$. By Lemma 8.12, the curve C indeed admits such an unramified cyclic degree 5 covering. Therefore there actually exists a unique curve X with real Weil polynomial equal to polynomial (3) in Theorem 2.4 and Proposition 8.2 follows. \square

9 Genus 7 optimal curves

Let E be the optimal genus 1 curve of affine equation $y^2 + y = x^3 + x$ described in Remark 3.4. In this last section we present a class field theoretic construction of a ray class field of $\mathbb{F}_2(E)$ whose proper quadratic subfields are function fields of optimal genus 7 curves. We show that the Zeta functions of these curves are not all the same, providing existence of at least two non-isomorphic genus 7 optimal curves over \mathbb{F}_2 .

Proposition 9.1. *Let K be the function field of E and let Q denote a degree 6 place of K of uniformizer $t = x^6 + x^5 + 1$. Let L be the ray class field of K of conductor $2Q$, in which all five rational points of K split completely. The Galois group $\mathcal{Gal}(L/K)$*

is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. The quadratic subfields of K are function fields of optimal genus 7 curves that do not all have the same Zeta function.



Proof. Let $a \in \mathbb{F}_{2^6}$ be a root of $x^6 + x^5 + 1$, and let Q be the place that consists of the point $(a, a^4 + a^3 + a^2 + 1)$ and its conjugates. The prime ideal corresponding to Q is $\mathfrak{p} = (x^6 + x^5 + 1, y + x^4 + x^3 + x^2 + 1)$. The principal divisor $(x^6 + x^5 + 1)$ is equal to $Q + Q' - 12P_0$ where Q' is the place consisting of $(a, a^4 + a^3 + a^2)$ and its conjugates. We take $t = x^6 + x^5 + 1$ as a uniformizer at Q . Denote by S the set of the five rational points of E described in Remark 3.4.

Let L be the ray class field of K of conductor $2Q$, in which all five rational points in S split completely. Then, by Artin reciprocity, the Galois group $G = \text{Gal}(L/K)$ is isomorphic to the quotient of $R = \mathbb{F}_{2^6}[[t]]^* / \{u : u \equiv 1 \pmod{t^2}\}$ by the image of the S -unit group O_S^* of K . A basis for O_S^* is given by the functions x , $x + 1$, y and $y + x$ having the following principal divisors

$$\begin{aligned} (x) &= P_1 + P_2 - 2P_0, \\ (x + 1) &= P_3 + P_4 - 2P_0, \\ (y) &= P_1 + 2P_3 - 3P_0, \\ (x + y) &= 2P_1 + P_4 - 3P_0. \end{aligned}$$

In order to compute the image of the S -units in R , we first observe that the image of the S -unit x has order 63 modulo t and hence it generates the 63-part of R . Then we compute

$$\begin{aligned} x^{63} - 1 &\equiv (x + 1)t && \pmod{t^2}, \\ (x + 1)^{63} - 1 &\equiv xt && \pmod{t^2}, \\ y^{63} - 1 &\equiv (x^5 + x^2)t && \pmod{t^2}, \\ (y + x)^{63} - 1 &\equiv (x^5 + x^4 + x^3 + x^2)t && \pmod{t^2}. \end{aligned}$$

Thus $\text{Gal}(L/K)$ is isomorphic to the quotient of $\mathbb{F}_2[x]/(x^6 + x^5 + 1)$ by the additive subgroup H generated by $x + 1$, x , $x^5 + x^2$ and $x^5 + x^4 + x^3 + x^2$. This is a quotient group of order 4 where all elements have order 2. Hence $\text{Gal}(L/K) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

The three subgroups of order 2 of $\text{Gal}(L/K)$ correspond to three coverings X_1 , X_2 and X_3 of E as in the diagram. Each curve X_i has ten rational points over \mathbb{F}_2 , since all five rational places of E split completely. Since the non-trivial characters of $\text{Gal}(L/K)$ have conductor $2Q$, the different of each quadratic extension $\mathbb{F}_2(X_i)/\mathbb{F}_2(E)$ has degree 12 and the three curves have genus 7 by the Hurwitz formula. Since $N_2(7) = 10$ by

Theorem 5 in [S1], they are three genus 7 optimal curves over \mathbb{F}_2 .

To show that the curves are not all isomorphic it suffices to consider the number of places of degree d of each curve X_i for $d \leq 4$. Since the rational points of E are all split and E has no places of degree 2 or 3, none of the three curves X_i has places of degree 2 or 3 either. Therefore a curve X_i can only have places of degree 4 if some places of E of degree 4 split completely in X_i . By class field theory, a place P of E splits completely in X_i if and only if the image of the uniformizer of P is trivial in the quotient R_i of R which is the ray class group of the covering $X_i \rightarrow E$. Consider the index 2 additive subgroups $H_1 = H + \langle x^3 \rangle$, $H_2 = H + \langle x^2 \rangle$ and $H_3 = H + \langle x^3 + x^2 \rangle$ of $\mathbb{F}_2[x]/(x^6 + x^5 + 1)$. The ray class group R_i associated to the curve X_i is isomorphic to the quotient group of $\mathbb{F}_2[x]/(x^6 + x^5 + 1)$ by H_i for $i = 1, 2, 3$. We present the results of the computation in Table 3. The first column lists for $j = 1, \dots, 5$ the

Q_j	$u_j(x, y)$	$g_j(x)$	H_i
Q_1	$y + x^3$	$x^5 + x$	H_2
Q_2	$y + x^3 + 1$	x^4	H_1
Q_3	$y + x^3 + x^2$	$x^5 + x^3 + x$	H_3
Q_4	$y + x^3 + x^2 + 1$	$x^4 + x^2$	H_3
Q_5	$x^2 + x + 1$	$x^5 + x^3 + x^2$	H_1

Table 3: Splitting behavior of the degree 4 places of E in each curve X_i .

degree 4 places Q_j of E as in Remark 3.4. In the second and third column we display the uniformizers $u_j(x, y)$'s of the Q_j 's and the images $g_j(x)$'s in $\mathbb{F}_2/(x^6 + x^5 + 1)$ of the $u_j(x, y)$'s. In other words we have $u_j(x, y)^{63} - 1 \equiv g_j(x)t \pmod{t^2}$. In the last column we write H_i for $i = 1, 2, 3$ whenever $g_j(x)$ belongs to H_i . The curve X_1 has four places of degree 4, since both Q_2 and Q_5 split. Similarly, also X_3 has four places of degree 4. On the other hand the curve X_2 has only two places of degree 4, since only Q_1 splits. Hence the two curves X_1 and X_2 are not isomorphic. \square

Remark 9.2. Let σ and τ be the automorphisms of E described in Remark 3.4. Then, the action of σ on the places of degree 6 of E listed in Remark 3.4, is given by

$$T_1 \mapsto T_9 \mapsto T_3 \mapsto T_4 \mapsto T_{10} \mapsto T_1.$$

Since the elliptic involution τ^2 switches T_9 and T_{10} we have that $\sigma^3\tau^2$ preserves T_{10} . In terms of adding points on the elliptic curve E one has $\sigma^3\tau^2 : (x, y) \mapsto (1, 1) - (x, y)$. A short computation shows that $\sigma^3\tau^2$ switches the functions x^3 and $x^2 + x^3$ modulo the subgroup H of $\mathbb{F}_2[x]/(x^6 + x^5 + 1)$. Therefore the curves X_1 and X_3 are actually isomorphic.

For completeness we compute the real Weil polynomials of the optimal genus 7 curves.

Proposition 9.3. For $i = 1, 2, 3$, the real Weil polynomial $h_i(t)$ and the vector $a(X_i)$

of the curve X_i are

$$\begin{aligned} h_{1,3}(t) &= (t+2)(t^6+5t^5+3t^4-15t^3-15t^2+9t+8), & a(X_{1,3}) &= [10, 0, 0, 4, 2, 5, 18, \dots], \\ h_2(t) &= (t+2)(t^2+3t+1)(t^4+2t^3-4t^2-5t+2), & a(X_2) &= [10, 0, 0, 2, 4, 11, 12, \dots]. \end{aligned}$$

Proof. By Remark 9.2 the curves X_1 and X_3 are isomorphic, therefore they have the same real Weil polynomial. In the proof of Proposition 9.1 we already observed that for the curves X_1 and X_2 one has $a_1 = 10$ and $a_2 = a_3 = 0$. We also proved that $a_4(X_1) = 4$ while $a_4(X_2) = 2$. Similarly to what was done for the places of degree 4, we consider the splitting behavior of the places of degree 5 of E listed in Remark 3.4 and display the results in Table 4.

$\mathbf{R_k}$	$\mathbf{u_k(x, y)}$	$\mathbf{g_k(x)}$	$\mathbf{H_i}$
R_1	$y + x^4$	$x^3 + x + 1$	H_1
R_2	$y + x^4 + 1$	$x^5 + x^4 + x$	H_3
R_3	$y + x^4 + x$	$x^4 + x^3 + x^2 + 1$	H_2
R_4	$y + x^4 + x + 1$	$x^5 + x^4 + x^3 + 1$	H_2

Table 4: Splitting behavior of the degree 5 places of E in each curve X_i .

Summing up we have $a_5(X_1) = 2$ and $a(X_2) = [10, 0, 0, 2, 4, \dots]$. Since the degree 6 place Q of E is the only ramifying place in each curve X_i , $i = 1, 2$, we have that $a_6(X_i)$ has to be odd, while $a_7(X_i)$ has to be even. We can now determine a parametric form for the real Weil polynomial of each curve X_i :

- i) For the curve X_1 the values of $\#X_1(\mathbb{F}_2) = a_1 = 10$, $a_2 = a_3 = 0$, $a_4 = 4$ and $a_5 = 2$ allow to determine the following parametric form:

$$h(t) = t^7 + 7t^6 + 13t^5 - 9t^4 - 45t^3 - 21t^2 + \alpha t + \beta.$$

One can check that only for the values of $(\alpha, \beta) = (26, 16)$ and $(\alpha, \beta) = (27, 18)$ all roots of $h(t)$ lie in the interval $[-2\sqrt{2}, 2\sqrt{2}]$. Only the first pair gives an odd number of degree 6 places, namely $a_6(X_1) = 5$. In this case $a_7(X_1) = 18$.

- ii) For the values $a(X_2) = [10, 0, 0, 2, 4, \dots]$ we have the parametric real Weil polynomial

$$h(t) = t^7 + 7t^6 + 13t^5 - 9t^4 - 47t^3 - 33t^2 + \alpha t + \beta.$$

In this case there are three pairs of values of (α, β) for which $h(t)$ has all roots in the interval $[-2\sqrt{2}, 2\sqrt{2}]$: the pair $(3, 2)$, which gives $a_6 = 10$; the pair $(4, 4)$, which gives $a_6 = 11$; and the pair $(5, 7)$, for which $a_6 = 12$. Hence the real Weil polynomial of X_2 corresponds to the unique pair $(\alpha, \beta) = (4, 4)$ for which a_6 is not even. In this case $a_7 = 12$.

□

References

- [A] R. Auer, *Ray class fields of global function fields with many rational places*, Acta Arith. **95** (2000), 97–122.
- [A-P] Y. Aubry and M. Perret, *Divisibility of zeta functions of curves in a covering*, Arch. Math. **82** (2004), 205–213.
- [G-V] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, Math. Comp. **69** (2000), 797–810. Updates at <http://www.manypoints.org/>
- [H] E. Howe, *Even sharper upper bounds on the number of points on curves*, slides based on work in progress with Kristin Lauter available at <http://alumnus.caltech.edu/~however/talks.html>.
- [H-L] E. Howe and K. Lauter, *Improved upper bounds for the number of points on curves over finite fields*, Ann. Inst. Fourier **53** (2003), 1677–1737.
- [L] K. Lauter, *Ray class field constructions of curves over finite fields with many rational points*, Algorithmic Number Theory, H. Cohen (ed.), Lecture Notes in Comput. Sci. **1122**, Springer, (1996), 187–195.
- [M-N] D. Maisner and E. Nart, with an appendix by E. Howe, *Abelian surfaces over finite fields as Jacobians*, Experimental Math. **11** (2002), 321–337.
- [N-X] H. Niederreiter and C.P. Xing, *Rational points on curves over finite fields: Theory and Applications*, London Mathematical Society Lecture Note Series 285, Cambridge, 2001.
- [S] J.-P. Serre, *Rational points on curves over finite fields*, unpublished notes by Fernando Q. Gouvêa of lectures at Harvard University, 1985.
- [S1] J.-P. Serre, *Sur le nombre des points rationnels d’une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris, Sér I Math. **296** (1983), 397–402; (= Oeuvres III, No. 128, 397–402).
- [Sch] R. Schoof, *Algebraic curves and coding theory*, UTM 336, Univ. of Trento, 1990.
- [Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
- [Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 2008.
- [W] A. Weil, *Zum Beweis des Torellischen Satzes*, Nachr. Akad. Göttingen, Math.-Phys. Kl., (1957), 33–53.

ALESSANDRA RIGATO

K.U. Leuven, Department of Mathematics,
 Celestijnenlaan 200 B, B-3001 Leuven (Heverlee), Belgium
 Alessandra.Rigato@wis.kuleuven.be